## IN THE CLAIMS

Please amend the claims as follows:

1. (Currently Amended) A cryptographically secure, computer hardware-implemented modular reduction method, comprising:

precomputing and storing in memory a constant U representing a bit-scaled reciprocal of a modulus M;

computing an estimated quotient value q for a number X to be reduced modulo M, wherein said computing is executed upon X in a computation unit by a multiplication by said constant U and by bit shifts of X and a shift of said multiplication;

generating in a random number generator a random error value E;

applying said generated random error value E to said estimated quotient value q to obtain a randomized quotient $q' = q - E$, wherein the random number generator has a specified error limit of one-half word, whereby $0 \leq E < (2^{w/2} - 1)$, with "w" being the word size of the computation unit in bits; and

calculating a remainder $R' = X - q'M$ in said computation unit, said remainder R' being larger than said modulus M but congruent to X modulo M.

2. (Original) The method of claim 1 wherein precomputing said constant U is performed according to the equation $U = [b^{2n+1}/M]$, where $b = 2^w$, with w being the word size of the computation unit in bits.

3. (Previously Presented) The method of claim 2 wherein computing the estimated quotient value q is performed by the computation unit according to the equation $q = [ ([X/b^n] \cdot U)/b^{n+2}]$.

4. (Currently Amended) The method of claim 3 wherein a supplemental subtraction by one is included in the computing of the estimated quotient value q.

5. (Original) The method of claim 1 wherein the modular reduction of X is part of a computer hardware-implemented cryptography program.

6. (Currently Amended) The method of claim 1 wherein an alternate calculation pathway is provided wherein generating and applying an error value to the estimated quotient value q may be selectively omitted.

7. (Cancelled)

8. (Currently Amended) Computational hardware for executing a cryptographically secure modular reduction method, the hardware comprising:

a computation unit adapted to perform word-wide multiply and accumulate steps on operands retrieved from a memory and carry terms from a set of registers;

a random number generator for generating a random error value E, wherein the random number generator has a specified error limit of one-half word, whereby $0 \leq E < (2^{w/2} - 1)$, with "w" being the word size of the computation unit in bits;

an operations sequencer comprising logic circuitry for controlling the computation unit and random number generator in accord with program instructions so as to carry out a modular reduction of a number X with respect to a modulus M that involves at least a computation of an estimated quotient value q from a pre-stored constant U representing a bit-scaled reciprocal of the modulus, a randomization of said estimated quotient value q with said random error value E to obtain a randomized quotient $q' = q - E$, and a calculation of a remainder value $R' = X - q'M$ .

9. (Original) The computation hardware of claim 8 further comprising operation parameter registers accessible by said operations sequencer, said registers containing any one or more of (a) pointers for locating operands within said memory, (b) information about lengths of operands, (c) carry injection control information for carry term registers, and (d) destination address information for intermediate results of operation steps.

10. (Original) The computation hardware of claim 8 wherein the pre-stored constant U in said memory is obtained from a precomputation according to the equation $U = [b^{2n+l}/M]$, where $b = 2^w$, with w being the word size of the computation unit in bits.

11. (Previously Presented) The computation hardware of claim 10 wherein the computation of said estimated quotient value q performed by said computation unit under control of said operations sequencer carrying out program instructions is done according to the equation $q = [ ( [X/b^n] \cdot U )/b^{n+2}]$.

12. (Currently Amended) The computation hardware of claim 11 wherein the computation of the estimated quotient value q performed by the computation unit includes a supplemental subtraction by one.

13. (Cancelled)

14. (Currently Amended) A ~~machine-readable medium stored on a computer~~ memory, comprising instructions, which when implemented by a processor, perform the following operations:

precomputing and storing in the memory a constant U representing a bit-scaled reciprocal of a modulus M;

computing an estimated quotient value q for a number X to be reduced modulo M, wherein said computing is executed upon X in a computation unit by a multiplication by said constant U and by bit shifts of X and a shift of said multiplication;

generating in a random number generator a random error value E;

applying said generated random error value E to said estimated quotient value q to obtain a randomized quotient $q' = q - E$, wherein the random number generator has a specified error limit of one-half word, whereby $0 \leq E < (2^{w/2} - 1)$, with "w" being the word size of the computation unit in bits; and

calculating a remainder $R' = X - q'M$ in said computation unit, said remainder R' being larger than said modulus M but congruent to X modulo M.

15. (Currently Amended) The ~~machine-readable medium~~ memory of claim 14, wherein precomputing said constant U is performed according to the equation $U = [b^{2n+1}/M]$, where $b = 2^w$, with w being the word size of the computation unit in bits.

16. (Currently Amended) The ~~machine-readable medium~~ memory of claim 15, wherein computing the estimated quotient value q is performed by the computation unit according to the equation $q = [ ([X/b^n] \cdot U)/b^{n+2}]$.

17. (Currently Amended) The ~~machine-readable medium~~ memory of claim 16 wherein a supplemental subtraction by one is included in the computing of the estimated quotient value q.

18. (Currently Amended) The ~~machine-readable medium~~ memory of claim 14, wherein the modular reduction of X is part of a computer hardware-implemented cryptography program.

19. (Currently Amended) The ~~machine-readable medium~~ memory of claim 14, wherein an alternate calculation pathway is provided wherein generating and applying an error value to the estimated quotient value q may be selectively omitted.

20. (New) The method of claim 1, comprising providing an alternate calculation pathway to selectively omit generating and applying an error value to the estimated quotient value q.